合肥工業大學

网络攻击实验报告

姓　　名　袁焕发

学　　号　2019217769

专业班级　物联网工程 19-2

指导教师　周健

院系名称　计算机与信息学院

2022 年 04 月 18 日

一、实验目的

1．MAC 地址洪泛

两台主机之间进行通信，通信内容和形式任意。第三台主机利用适当的洪泛工具发动 MAC 地址洪泛，并利用 Wireshark 抓包进行侦听。

2．ARP 中间人攻击

两台主机之间进行通信，通信内容和形式任意，第三台主机利用适当的 ARP 攻击工具发动 ARP 中间人攻击，并利用 Wireshark 抓包进行侦听。

二、实验环境

Windows7 虚拟机、Windows xp 虚拟机、kali 虚拟机、软件：Wireshark、Ettercap

三、实验原理

1．MAC 地址洪泛原理

攻击者利用交换机对于未知单播帧洪泛的原理，对流量进行抓取，以达到网络信息收集的目的。 首先攻击者会向交换机中发送大量的虚假 MAC 地址，将交换机中的 CAM 表填满,这样其他主机所发送的数据帧交换机会做洪泛处理，攻击者自己的主机就可以接收到受害者的数据帧，攻击者只需要使用抓包软件就可以获取相应的信息。

2．ARP 中间人攻击原理

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的网络层，负责将某个 IP 地址解析成对应的 MAC 地址。

ARP 病毒攻击是局域网最常见的一种攻击方式。由于 TCP/IP 协议存在的一些漏洞给 ARP 病毒有进行欺骗攻击的机会，ARP 利用 TCP/IP 协议的漏洞进行欺骗攻击，现已严重影响到人们正常上网和通信安全。当局域网内的计算机遭到 ARP 的攻击时，它就会持续地向局域网内所有的计算机及网络通信设备发送大量的 ARP 欺骗数据包，如果不及时处理，便会造成网络通道阻塞、网络设备的承载过重、网络的通讯质量不佳等情况。

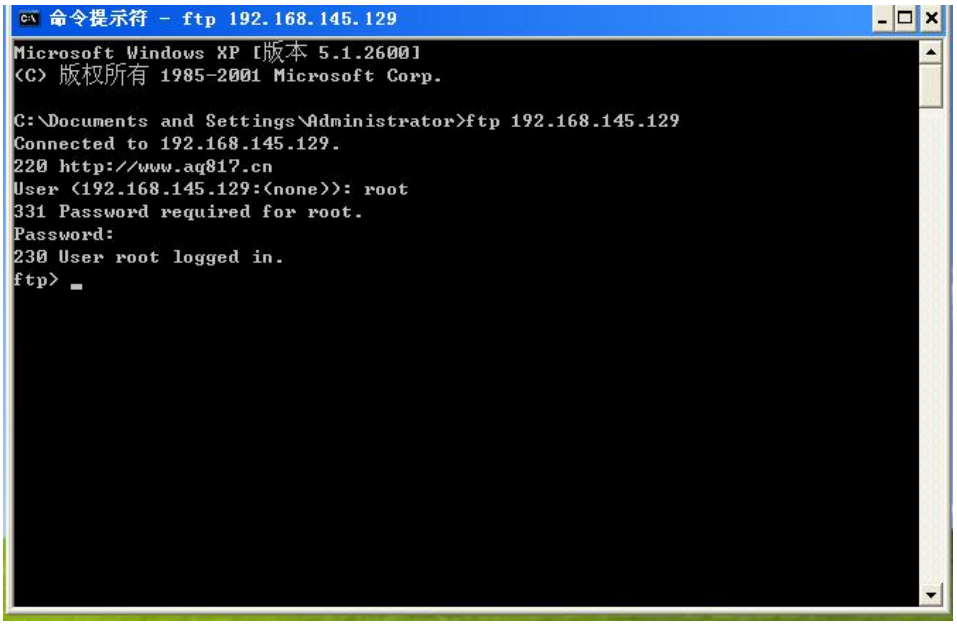
ARP 攻击主要是通过伪造 IP 地址和 MAC 地址进行欺骗。使以太网数据包的源地址、目标地址和 ARP 数通信量导致网络中断或中间人攻击。ARP 攻击主要存在于局域网中。若其中一台计算机感染 ARP 病毒。就会试图通过 ARP 欺骗截获局域网内其他计算机的信息，造成局域网内的计算机通信故障。

四、实验步骤

1．MAC 地址洪泛

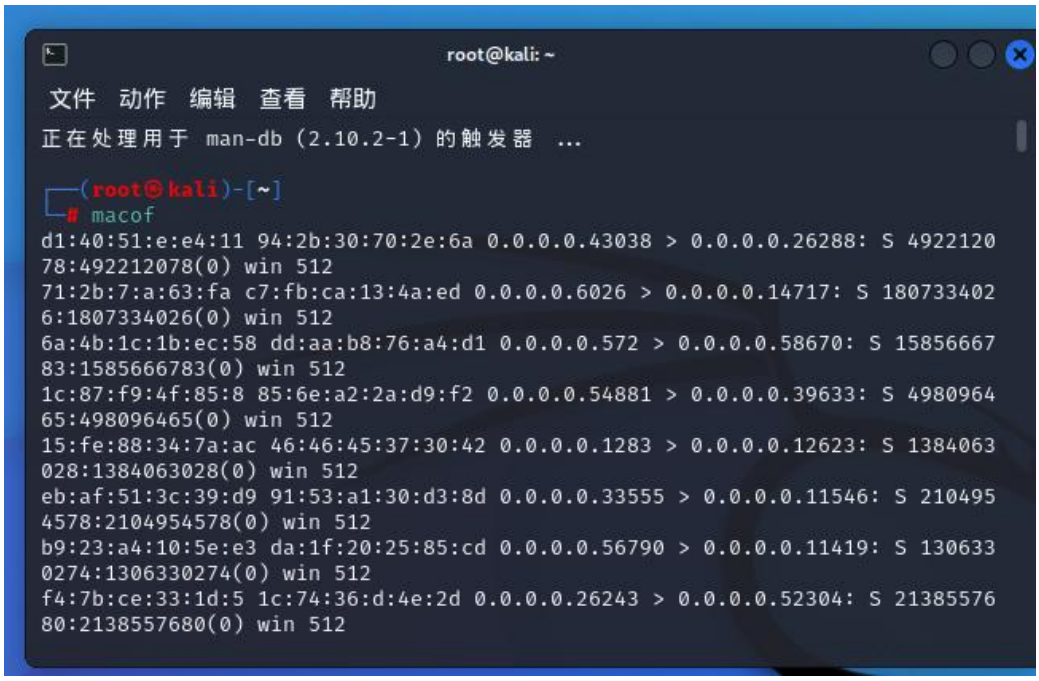
首先建立 FTP 服务器，服务器地址 192.168.145.129

接着在另一台虚拟机上连接服务器，测试连通性。

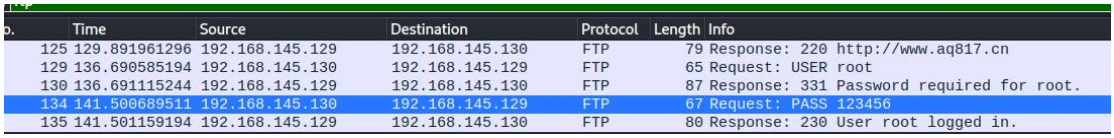


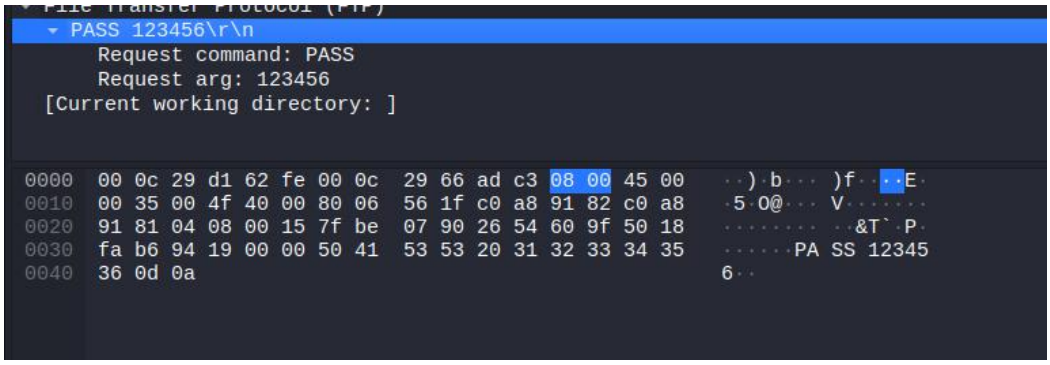
连接成功，断开连接。

Kali 虚拟机开始进行 mac 地址洪泛



然后此时建立 FTP 服务器连接，同时使用 Wireshark 抓包。

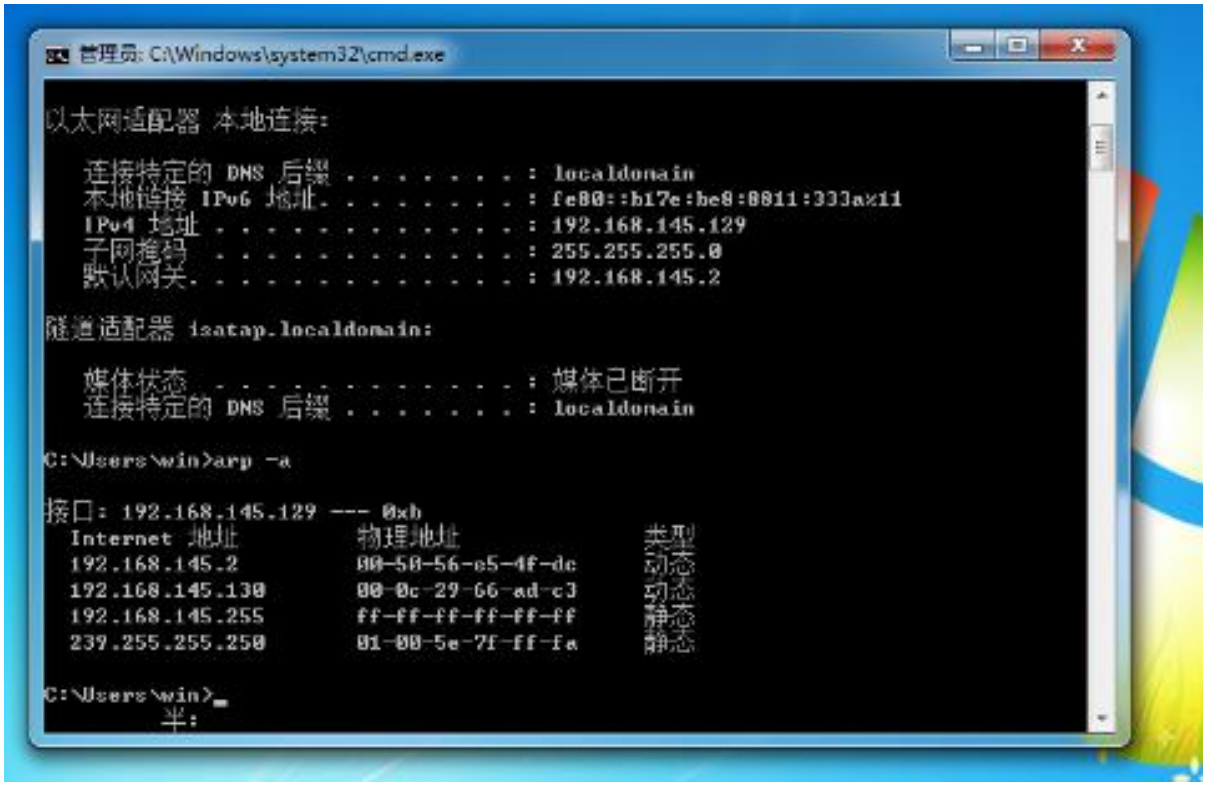


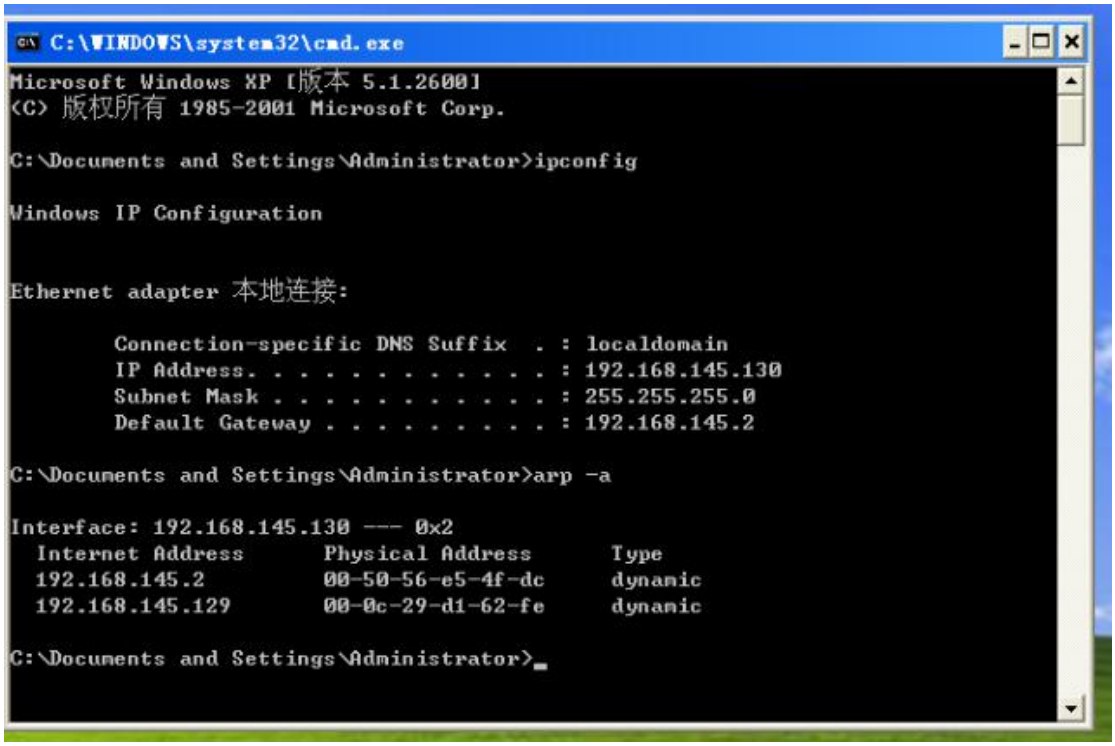


成功抓取到密码信息。

2. ARP 中间人攻击

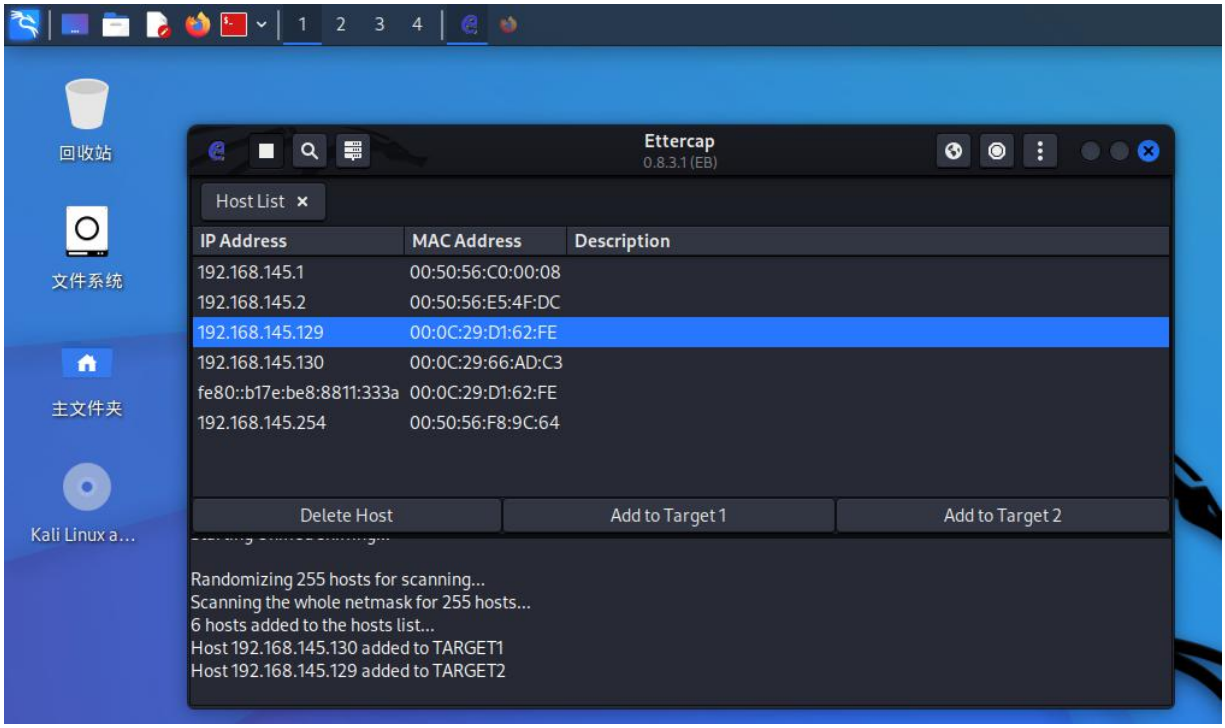
正常状态下两台客户机的 IP 和 MAC 地址。



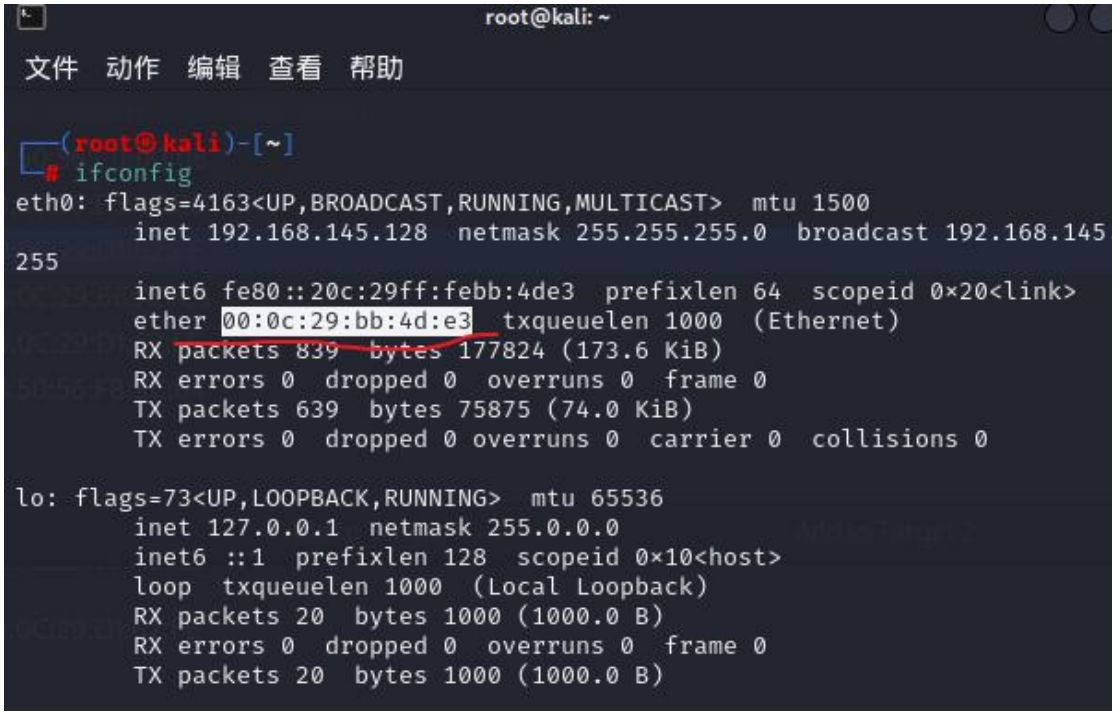


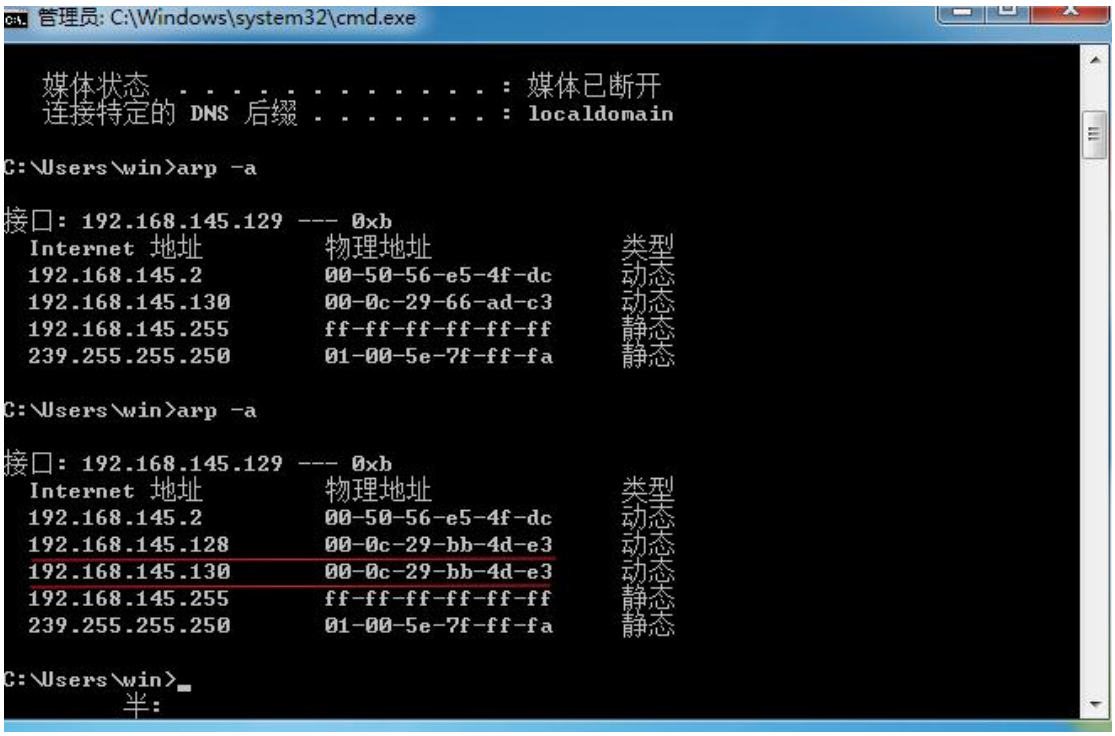
首先依然是建立 FTP 服务器

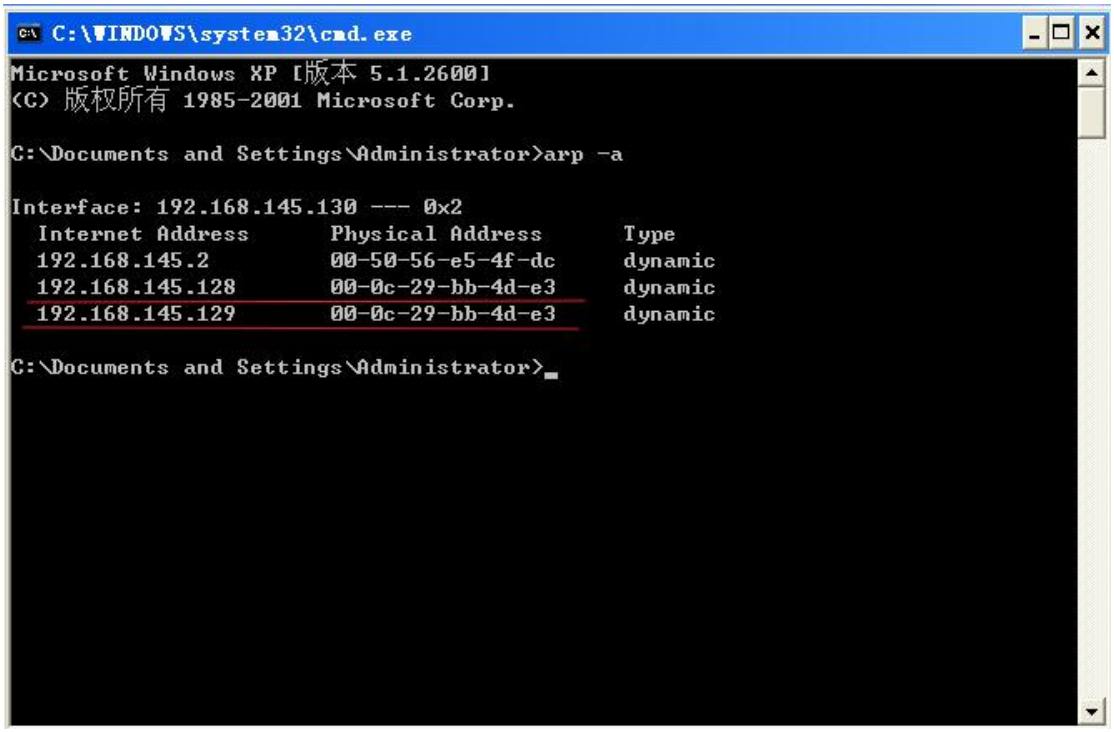
然后用 kali 虚拟机作为中间人进行攻击，将两台客户机地址分别加入 Target1 和 Target2，然后启动攻击。



192.168.145.128 是 kali 虚拟机 IP 地址，192.168.145.129 是 FTP 服务器地址，192.168.145.130 是客户机所在地址。

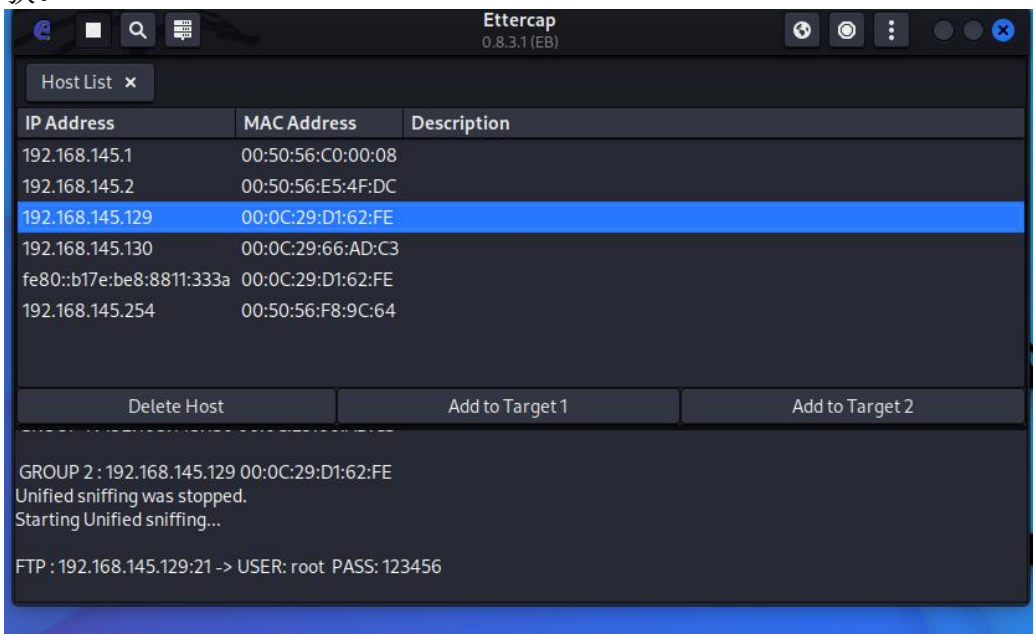

root@kali: ~
文件 动作 编辑 查看 帮助
(root㉿kali)-[~]
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.145.128 netmask 255.255.255.0 broadcast 192.168.145
255
inet6 fe80::20c:29ff:febb:4de3 prefixlen 64 scopeid 0×20<link>
ether 00:0c:29:bb:4d:e3 txqueuelen 1000 (Ethernet)
RX packets 839 bytes 177824 (173.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 639 bytes 75875 (74.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 20 bytes 1000 (1000.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1000 (1000.0 B)


管理员: C:\Windows\system32\cmd.exe
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . : localdomain
C:\Users\win>arp -a
接口: 192.168.145.129 --- 0xb
Internet 地址 物理地址 类型
192.168.145.2 00-50-56-e5-4f-dc 动态
192.168.145.130 00-0c-29-66-ad-c3 动态
192.168.145.255 ff-ff-ff-ff-ff-ff 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态
C:\Users\win>arp -a
接口: 192.168.145.129 --- 0xb
Internet 地址 物理地址 类型
192.168.145.2 00-50-56-e5-4f-dc 动态
192.168.145.128 00-0c-29-bb-4d-e3 动态
192.168.145.130 00-0c-29-bb-4d-e3 动态
192.168.145.255 ff-ff-ff-ff-ff-ff 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态
C:\Users\win>
半:



攻击之后可以看到 kali 虚拟机的 MAC 地址已经变成了和 FTP 服务器所在 MAC 地址相同。

此时客户机进行 FTP 服务器连接操作，向服务器传输的报文信息已经被中间人截获。



五、实验总结

这次实验我通过查阅资料完成了网络攻击实验，明白了网络攻击的手段原理，知道了网络安全的重要性。